UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/588,128	07/11/2007	Tomoyuki Asano	294253US8PCT	3844

22850 7590 04/01/2009

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
04/01/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/588,128	ASANO, TOMOYUKI	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 February 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/588,128 is presented for examination by the examiner. Claims 1-22 have been amended and have been examined.

Response to Amendment

Specification

Examiner acknowledges Applicant wishes to hold in abeyance correction of the title.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claims 1-22, the claims are generally narrative and indefinite, failing to conform to current U.S. practice. They appear to be a literal translation into English from a foreign document. The wording makes examination very difficult to determine the metes and bounds of the claims. Phrases such as “service providing server for

executing service providing processing" are unnecessarily ambiguous and confusing. Appropriate correction is required. The currently filed amendment has corrected some of the previous problems but not all of them. Particularly claim 1 still has the problem mentioned explicitly is the last Office Action. Claim 1 declares a service providing server meaning a server which provides a service. The service provided is not definitively recited. The claim then declares the server is for executing service providing processing. This phrase is confusing all by itself. It appears the claim is defining a server that provides a response to service request from an apparatus and the server comprises the limitation recited in the body of the claim. However there are too many unnecessary words in the claim to definitely interpret the scope as such.

As per claims 21 and 22, the preamble declaration is indefinite. There seems to be a contradiction in what is being claimed. The preamble first recites a data processing method. Then the preamble states that the method is for executing service providing processing. The indefiniteness stems from the contradiction between data processing and service providing processing. Is the claim directed to processing data or processing service requests? Appropriate correction is required.

Response to Arguments

Applicant's arguments with respect to independent claims 6, 16, and 22 have been considered but are moot in view of the new ground(s) of rejection.

Applicant's arguments with respect to independent claims 1, 11, and 21 have been fully considered but they are not persuasive. Turning to claim 1 which shares common limitations to 11 and 21, Applicant has alleged that the Kii reference fails to teach or suggest a requested service is permitted based on acquired service providing situation data. Examiner has interpreted the functionality of Kii to achieve the same underlying result as the claimed invention. Kii uses different terms to describe the features but the process is the same. Both Kii and the claims use the term medium ID. The title-unique values of the claims correspond to the access right information of the Kii because the titles each have own respective access right information. The claimed invention recites that these title-unique values having corresponding service providing situation data. Examiner interprets this term has just data which is expressed for each title-unique value. This is similar to having a unique table with its own data. One would find the table which corresponds to the content and check within the table to determine how to handle relevant situation. Kii teaches the same process with the access rights information (0018). Inside the access right information, inherently are conditions or permissions which determine how the system responds to situations. The claimed invention then uses this data to determine if a requested service should be permitted. Kii teaches this limitation as well (0118 and 0122). Kii teaches only the relevant service is provided based on the access right information. Kii does not explicitly give the data in the access right information a separate name but the data is there because it is used to check is a requested service is permissible or not.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 2, 5, 11, 12, 15, and 21 are rejected under 35 U.S.C. 102(b) as being anticipated by USP Application Publication 2002/0099661 to Kii et al., hereinafter Kii.

As per claim 1, Kii teaches a service providing server for executing service providing processing in response to a service providing request from an information processing apparatus, characterized by having:

a data reception section which receives a service request accompanied by an information recording medium ID [ID] and a service ID [connection program and information identifying the service provider's ID], from the information processing apparatus (0113);

a storage section [database] which stores service providing situation data [Fig 6, upload/download rights] for each of the information recording medium IDs as service management data for each of title-unique values [access right information] corresponding to titles of content stored on information recording media (0113);

and a data processing section which executes processing of verifying the information recording medium ID received via the data reception section, acquires a title-unique value on the basis of the information recording medium ID on condition that the information recording medium ID is validated (0017), acquires service providing situation data corresponding to the title-unique value from the storage section to judge whether or not a service specified by the information recording medium ID and the service ID is providable, and executes the service providing processing on condition that the service is judged to be providable (0118).

As per claim 2, Kii teaches the data processing section is configured to execute the processing of verifying the information recording medium ID as processing of verifying signature data contained in the information recording medium ID, and execute the processing of acquiring, from the storage section, the service providing situation data corresponding to the title-unique value, according to the title-unique value contained in the information recording medium ID, or the title-unique value calculated by executing a calculation based on data contained in the information recording medium ID (0018).

As per claim 5, Kii teaches a prime set [unique ID] in response to each of a number of information recording media manufactured (0007); and

data IDKey [encryption key] calculated by a calculation based on the prime and the title-unique value [ID] (0118); and

the data processing section is configured to execute processing of judging whether or not data contained in the information recording medium ID is the prime, as

the ID verifying processing, and also calculate the title-unique value from the data IDKey contained in the information recording medium ID, and acquiring the service providing situation data corresponding to the title-unique value calculated, from the storage section (0118). For purposes of examination is appears this claim is directed to the idea that each medium ID has the necessary parameters to perform public key encryption to authenticate the mediums with the server. The prime set can be interpreted to be those known and necessary parameters that two or more parties must agree on to perform public key encryption. A choice of a prime could be interpreted as a private key. Therefore the IDkey would be the encrypted form of the unique media ID (aka digital signature}. This would be passed to the server to prove one's authenticity. Kii teaches a public key authentication process and as such Examiner finds nothing novel to the notion of public key cryptography in this claim.

As per claim 11, Kii teaches a data processing method for executing service providing processing in response to a service providing request from an information processing apparatus, characterized by having:

a data reception section which receives a service request accompanied by an information recording medium ID [ID] and a service ID [connection program and information identifying the service provider's ID], from the information processing apparatus (0113);

a storage section [database] which stores service providing situation data [Fig 6, upload/download rights] for each of the information recording medium IDs as service

management data for each of title-unique values [access right information] corresponding to titles of content stored on information recording media (0113);

and a data processing section which executes processing of verifying the information recording medium ID received via the data reception section, acquires a title-unique value on the basis of the information recording medium ID on condition that the information recording medium ID is validated (0017), acquires service providing situation data corresponding to the title-unique value from the storage section to judge whether or not a service specified by the information recording medium ID and the service ID is providable, and executes the service providing processing on condition that the service is judged to be providable (0118).

As per claim 12, Kii teaches the data processing section is configured to execute the processing of verifying the information recording medium ID as processing of verifying signature data contained in the information recording medium ID, and execute the processing of acquiring, from the storage section, the service providing situation data corresponding to the title-unique value, according to the title-unique value contained in the information recording medium ID, or the title-unique value calculated by executing a calculation based on data contained in the information recording medium ID (0018).

As per claim 15, Kii teaches a prime set [unique ID] in response to each of a number of information recording media manufactured (0007); and

data IDKey [encryption key] calculated by a calculation based on the prime and the title-unique value [ID] (0118); and

the data processing section is configured to execute processing of judging whether or not data contained in the information recording medium ID is the prime, as the ID verifying processing, and also calculate the title-unique value from the data IDKey contained in the information recording medium ID, and acquiring the service providing situation data corresponding to the title-unique value calculated, from the storage section (0118). For purposes of examination is appears this claim is directed to the idea that each medium ID has the necessary parameters to perform public key encryption to authenticate the mediums with the server. The prime set can be interpreted to be those known and necessary parameters that two or more parties must agree on to perform public key encryption. A choice of a prime could be interpreted as a private key. Therefore the IDkey would be the encrypted form of the unique media ID (aka digital signature}. This would be passed to the server to prove one's authenticity. Kii teaches a public key authentication process and as such Examiner finds nothing novel to the notion of public key cryptography in this claim.

As per claim 21, Kii teaches a program for executing service providing processing in response to a service providing request from an information processing apparatus, characterized by having:

a data reception section which receives a service request accompanied by an information recording medium ID [ID] and a service ID [connection program and information identifying the service provider's ID], from the information processing apparatus (0113);

a storage section [database] which stores service providing situation data [Fig 6, upload/download rights] for each of the information recording medium IDs as service management data for each of title-unique values [access right information] corresponding to titles of content stored on information recording media (0113);

and a data processing section which executes processing of verifying the information recording medium ID received via the data reception section, acquires a title-unique value on the basis of the information recording medium ID on condition that the information recording medium ID is validated (0017), acquires service providing situation data corresponding to the title-unique value from the storage section to judge whether or not a service specified by the information recording medium ID and the service ID is providable, and executes the service providing processing on condition that the service is judged to be providable (0118).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3, 4, 13, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kii in view of USP Application Publication 2003/0221097 to Nakano et al., hereinafter Nakano.

As per claims 3 and 13, Kii teaches a server contains a storage section for holding a holding a database filled with the unique media IDs (0007). Kii is silent in disclosing that the server stores a revocation list being a list of unauthorized information recording medium IDs; and the processing of verifying the information recording medium ID in the data processing section is executed as processing of comparing the information recording medium ID received from the information processing apparatus with the IDs recorded in the revocation list. Nakano teaches revocation list being a list of unauthorized information recording medium IDs; and the processing of verifying the information recording medium ID in the data processing section is executed as processing of comparing the information recording medium ID received from the information processing apparatus with the IDs recorded in the revocation list (0017). Kii teaches the use of public key authentication for recorded media. Nakano also teaches the use of public key authentication for recorded media, but also teaches the use of a revocation list to flag compromised media. Kii does not teach a method to combat illegal copies of media. Revocation lists are a known method to combat illegal copies. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Kii with those of Nakano to not allow user's of illegal copies from gaining access to content on the server.

As per claims 4 and 14, Kii teaches the information recording medium ID is configured to include a title-unique value [access right information] corresponding to a title of content stored in an information recording medium, (0128); and
the data processing section is configured to execute the processing of verifying the information recording medium ID; and also execute the processing of acquiring the service providing situation data corresponding to the title-unique value contained in the information recording medium ID, from the storage section [database] (0128). Kii teaches the use of public key encryption as an alternate means to authentication the unique media but stops short of teaching the generation of signature data and comparing the signature data to in the medium ID (0128). Nakano teaches in more detail the use of public key cryptography for creating signature messages and verifying them with public key information as a means of authentication (0047). The use of public key cryptography is well known and established in the art. Kii even suggests using it. Nakano gives the details of how public key cryptography is applied to signatures for authentication. Substituting known methods for similar purposes yielding predictable results is within the capabilities of one of ordinary skill in the art. Therefore the claim would have been obvious because generating messages and authentication [comparing] them with the use of public keys is known in the art.

Claims 6, 7, 10, 16, 17, 20, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kii in view of USP Application Publication 2002/0129262 to Kutaragi et al., hereinafter Kutaragi.

As per claim 6, Kii teaches an information processing apparatus (0165) for executing a service providing request to a service providing server, characterized by having:

a recording medium interface which executes processing of accessing an information recording medium (0256); and

a data processing section which executes processing of verifying an information recording medium ID read from the information recording medium via the recording medium interface, and executes processing of transmitting the information recording medium ID to the service providing server on condition that the information recording medium ID is validated (0392-0394). Kii does not explicitly teach first verifying the medium ID before transmitting it to the service providing server. Kutaragi teaches this limitation in paragraph 0078 and 0079. Kutaragi teaches the apparatus can first check and verifying the medium ID is proper before sending it to the server for further processing. It is obvious to one of ordinary skill in the art to substitute known method which yield predictable results. By verifying the medium ID before requesting service by the server, the server can avoid requests from illegal mediums. This would cut down on the processing performed by the server and free its resources for legitimate requests. The capabilities of one of ordinary skill in the art include the substitution of known methods.

As per claim 7, Kii teaches the data processing section is configured to execute the processing of verifying the information recording medium ID as processing of verifying signature data contained in the information recording medium ID, and execute

the processing of acquiring, from the storage section, the service providing situation data corresponding to the title-unique value, according to the title-unique value contained in the information recording medium ID, or the title-unique value calculated by executing a calculation based on data contained in the information recording medium ID (0018). Using the combination as described in the rejection of claim 6, this type of processing could then be performed by the apparatus before sending the request to the server.

As per claim 10, Kii teaches a prime set [unique ID] in response to each of a number of information recording media manufactured (0007); and

data IDKey [encryption key] calculated by a calculation based on the prime and the title-unique value [ID] (0118); and

the data processing section is configured to execute processing of judging whether or not data contained in the information recording medium ID is the prime, as the ID verifying processing, and also calculate the title-unique value from the data IDKey contained in the information recording medium ID, and acquiring the service providing situation data corresponding to the title-unique value calculated, from the storage section (0118). For purposes of examination is appears this claim is directed to the idea that each medium ID has the necessary parameters to perform public key encryption to authenticate the mediums with the server. The prime set can be interpreted to be those known and necessary parameters that two or more parties must agree on to perform public key encryption. A choice of a prime could be interpreted as a private key. Therefore the IDkey would be the encrypted form of the unique media ID

(aka digital signature}. This would be passed to the server to prove one's authenticity. Kii teaches a public key authentication process and as such Examiner finds nothing novel to the notion of public key cryptography in this claim.

As per claim 16, Kii teaches a data processing method (0165) for executing a service providing request to a service providing server, characterized by having:

a recording medium interface which executes processing of accessing an information recording medium (0256); and

a data processing section which executes processing of verifying an information recording medium ID read from the information recording medium via the recording medium interface, and executes processing of transmitting the information recording medium ID to the service providing server on condition that the information recording medium ID is validated (0392-0394). Kii does not explicitly teach first verifying the medium ID before transmitting it to the service providing server. Kutaragi teaches this limitation in paragraph 0078 and 0079. Kutaragi teaches the apparatus can first check and verifying the medium ID is proper before sending it to the server for further processing. It is obvious to one of ordinary skill in the art to substitute known method which yield predictable results. By verifying the medium ID before requesting service by the server, the server can avoid requests from illegal mediums. This would cut down on the processing performed by the server and free its resources for legitimate requests. The capabilities of one of ordinary skill in the art include the substitution of known methods.

As per claim 17, Kii teaches the data processing section is configured to execute the processing of verifying the information recording medium ID as processing of verifying signature data contained in the information recording medium ID, and execute the processing of acquiring, from the storage section, the service providing situation data corresponding to the title-unique value, according to the title-unique value contained in the information recording medium ID, or the title-unique value calculated by executing a calculation based on data contained in the information recording medium ID (0018). Using the combination as described in the rejection of claim 6, this type of processing could then be performed by the apparatus before sending the request to the server.

As per claim 20, Kii teaches a prime set [unique ID] in response to each of a number of information recording media manufactured (0007); and

data IDKey [encryption key] calculated by a calculation based on the prime and the title-unique value [ID] (0118); and

the data processing section is configured to execute processing of judging whether or not data contained in the information recording medium ID is the prime, as the ID verifying processing, and also calculate the title-unique value from the data IDKey contained in the information recording medium ID, and acquiring the service providing situation data corresponding to the title-unique value calculated, from the storage section (0118). For purposes of examination is appears this claim is directed to the idea that each medium ID has the necessary parameters to perform public key encryption to authenticate the mediums with the server. The prime set can be

interpreted to be those known and necessary parameters that two or more parties must agree on to perform public key encryption. A choice of a prime could be interpreted as a private key. Therefore the IDkey would be the encrypted form of the unique media ID (aka digital signature}. This would be passed to the server to prove one's authenticity. Kii teaches a public key authentication process and as such Examiner finds nothing novel to the notion of public key cryptography in this claim.

As per claim 22, Kii teaches a program (0165) for executing a service providing request to a service providing server, characterized by having:

a recording medium interface which executes processing of accessing an information recording medium (0256); and

a data processing section which executes processing of verifying an information recording medium ID read from the information recording medium via the recording medium interface, and executes processing of transmitting the information recording medium ID to the service providing server on condition that the information recording medium ID is validated (0392-0394). Kii does not explicitly teach first verifying the medium ID before transmitting it to the service providing server. Kutaragi teaches this limitation in paragraph 0078 and 0079. Kutaragi teaches the apparatus can first check and verifying the medium ID is proper before sending it to the server for further processing. It is obvious to one of ordinary skill in the art to substitute known method which yield predictable results. By verifying the medium ID before requesting service by the server, the server can avoid requests from illegal mediums. This would cut down on

the processing performed by the server and free its resources for legitimate requests. The capabilities of one of ordinary skill in the art include the substitution of known methods.

Claims 8, 9, 18, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kii and Kutaragi as applied to claims 6 and 16 above, and further in view of Nakano.

As per claims 8 and 18, Kii teaches a server contains a storage section for holding a holding a database filled with the unique media IDs (0007). Kii and Kutaragi are silent in disclosing that the server stores a revocation list being a list of unauthorized information recording medium IDs; and the processing of verifying the information recording medium ID in the data processing section is executed as processing of comparing the information recording medium ID received from the information processing apparatus with the IDs recorded in the revocation list. Nakano teaches revocation list being a list of unauthorized information recording medium IDs; and the processing of verifying the information recording medium ID in the data processing section is executed as processing of comparing the information recording medium ID received from the information processing apparatus with the IDs recorded in the revocation list (0017). Kii teaches the use of public key authentication for recorded media. Nakano also teaches the use of public key authentication for recorded media, but also teaches the use of a revocation list to flag compromised media. Kii does not teach a method to combat illegal copies of media. Revocation lists are a known method

to combat illegal copies. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Kii and Kutaragi with those of Nakano to not allow user's of illegal copies from gaining access to content on the server.

As per claims 9 and 19, Kii teaches the information recording medium ID is configured to include a title-unique value [access right information] corresponding to a title of content stored in an information recording medium, (0128); and
the data processing section is configured to execute the processing of verifying the information recording medium ID; and also execute the processing of acquiring the service providing situation data corresponding to the title-unique value contained in the information recording medium ID, from the storage section [database] (0128). Kii teaches the use of public key encryption as an alternate means to authentication the unique media but stops short of teaching the generation of signature data and comparing the signature data to in the medium ID (0128). Nakano teaches in more detail the use of public key cryptography for creating signature messages and verifying them with public key information as a means of authentication (0047). The use of public key cryptography is well known and established in the art. Kii even suggests using it. Nakano gives the details of how public key cryptography is applied to signatures for authentication. Substituting known methods for similar purposes yielding predictable results is within the capabilities of one of ordinary skill in the art. Therefore the claim

would have been obvious because generating messages and authentication [comparing] them with the use of public keys is known in the art.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2431